



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/042,652	01/08/2002	Jeffrey Bruce Lotspeich	ARC920010090US1	7388
7590	03/25/2008		EXAMINER	
John L. Rogitz Rogitz & Associates 750 B Street, Suite 3120 San Diego, CA 92101			WYSZYNSKI, AUBREY H	
			ART UNIT	PAPER NUMBER
			2134	
			MAIL DATE	DELIVERY MODE
			03/25/2008	PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

---

BEFORE THE BOARD OF PATENT APPEALS  
AND INTERFERENCES

---

*Ex parte* JEFFREY BRUCE LOTSPIECH, DALIT NAOR, SIGFREDO  
ISMAEL NIN, and FLORIAN PESTONI

---

Appeal 2007-3454  
Application 10/042,652<sup>1</sup>  
Technology Center 2100

---

Decided: March 25, 2008

---

Before JOSEPH L. DIXON, ALLEN R. MACDONALD, and  
JEAN R. HOMERE, *Administrative Patent Judges*.

HOMERE, *Administrative Patent Judge*.

DECISION ON APPEAL

---

<sup>1</sup> Filed on Jan. 08, 2002. The real party in interest is International Business Machines Corp.

## I. STATEMENT OF CASE

Appellants appeal under 35 U.S.C. § 134 from the Examiner's final rejection of claims 1, 3 through 16, 23 through 25, and 28 through 48. Claims 2, 26, and 27 have been canceled. We have jurisdiction under 35 U.S.C. § 6(b). We affirm-in-part, and we enter new grounds of rejection.

According to Appellants, as depicted in Figures 1 and 3, the invention relates to a method and system for securely transmitting over the Internet data stream between a content owner (16), a subscription provider (14) and a device player (12). (Spec. 9-10.) Particularly, the content owner (16) or subscriber service provider (14) utilizes a title key to encrypt an outgoing data stream. The subscriber service provider (14) then uses an encryption function to encrypt the title key with a channel-unique key by combining a channel key and a session key. (*Id.* 11-12.) Upon receiving the encrypted data stream, the device player (12) uses a device key to decrypt the session key, which is used in turn to decrypt the channel unique key to thereby derive the title key. Subsequently, the player (12) uses the title key to decrypt the content of the multicast data. (*Id.* 15.)

Independent claims 1 and 41 are illustrative of the invention. They read as follows:

1. A method for securely transmitting multicast data, comprising:
  1. encrypting at least one title T with at least title key  $K_T$ ; and
  2. encrypting the title key  $K_T$  with at least one channel-unique key  $K_{cu}$  using at least one encryption function S to render a multicast data channel

encrypted as  $S_{K_{cu}}(K_T)$ ,  $S_{KT}(T)$ , wherein the channel-unique key  $K_{cu}$  is the result of a combination of a channel key  $K_c$  and a session key  $K_s$ .

41. A player for decrypting streamed content, comprising:
  - at least one device key  $K_d$ ;
  - means for decrypting a session key  $K_s$  using the device key  $K_d$ ;
  - means for decrypting a channel unique key  $K_{cu}$  using at least the session key  $K_s$  ; and
  - means for deriving a title key  $K_T$  using at least the channel unique key  $K_{cu}$  the title key  $K_T$  being useful for decrypting content.

The Examiner relied on the following prior art in rejecting the claims on appeal:

Knauft	US2001/0029581A1	Oct. 11, 2001
Ishiguro	US2002/0083319A1	Jun. 27, 2002 (filed Apr. 14, 1998)
Richards	US 6,690,795B1	Feb. 10, 2004 (filed Mar. 4, 1997)
Yokota	US 6,691,149B1	Feb. 10, 2004 (filed Mar. 30, 2000)

The Examiner rejected the claims<sup>2</sup> on appeal as follows:

1. Claims 41-46 stand rejected under 35 U.S.C. § 102 as being anticipated by Richards.
2. Claims 1, 3-16, 23, and 47 stand rejected under 35 U.S.C. § 103 as being unpatentable over any of Yokota, Knauft, and Richards in

---

<sup>2</sup> Claims 17 through 22 were rejected under non-statutory double patenting. The Examiner indicated that the Terminal Disclaimer was not accepted at page 2 of the Answer, but did not repeat the rejection in the Answer. Therefore, this rejection is not on appeal before us.

combination with Ishiguro.

3. Claims 24, 25, 28 through 40, and 48 stand rejected under 35 U.S.C. § 103 as being unpatentable over the combination of Richards with Ishiguro.

#### FINDINGS OF FACT

The following findings of fact (FF) are supported by a preponderance of the evidence.

##### *Richards*

1. Richards discloses a method/ system that combines a plurality of keys to produce a segment key (SK) for encrypting and decrypting streamed television content transmitted to customers. (Col. 1, ll. 21-23.)

2. In a first embodiment, the segment key (SK) is obtained by using a program key (PK) that is encrypted with a unique customer code. (Col. 9, ll. 12-18.) Richards discloses that PK and SK change over time. (Col. 9, ll. 32, 53.)

3. In a second embodiment, the unique customer code is replaced with a user encryption variable (UEV), which is used to produce a channel access key (CAK). The CAK in turn is used to produce a control channel key (CCK). The CCK is in turn used to produce the program Key, which in turn is used to produce the segment key (SK) that is used to encrypt or decrypt content data. Richard discloses that all of these keys, except the UEV, change over time. (Col. 11, ll. 1-37.)

##### *Ishiguro*

As acknowledged by Appellants (App. Br. 7), Ishiguro discloses a personal computer that generates a common session key by combining two encrypted source session keys received from a DVD player. (pp. 6, para. 0091-0096.)

PRINCIPLES OF LAW  
OBVIOUSNESS

Appellants have the burden on appeal to the Board to demonstrate error in the Examiner's position. *See In re Kahn*, 441 F.3d 977, 985-86 (Fed. Cir. 2006) ("On appeal to the Board, an applicant can overcome a rejection [under § 103] by showing insufficient evidence of *prima facie* obviousness or by rebutting the *prima facie* case with evidence of secondary indicia of nonobviousness.") (quoting *In re Rouffet*, 149 F.3d 1350, 1355 (Fed. Cir. 1998)).

The Supreme Court in *Graham v. John Deere Co.*, 383 U.S. 1, 17-18 (1966), stated that the following factual inquiries underpin any determination of obviousness:

Under § 103, [1] the scope and content of the prior art are to be determined; [2] differences between the prior art and the claims at issue are to be ascertained; and [3] the level of ordinary skill in the pertinent art resolved. Against this background, the obviousness or nonobviousness of the subject matter is determined. Such (4) secondary considerations as commercial success, long felt but unsolved needs, failure of others, etc., might be utilized to give light to the circumstances surrounding the origin of the subject matter sought to be patented. As indicia of obviousness or nonobviousness, these inquiries may have relevancy.

Where the claimed subject matter involves more than the simple substitution of one known element for another or the mere application of a known technique to a piece of prior art ready for the improvement, a holding of obviousness must be based on “an apparent reason to combine the known elements in the fashion claimed.” *KSR Int'l v. Teleflex, Inc.*, 127 S. Ct. 1727, 1740-41 (2007). That is, “there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness.” *Id.*, 127 S. Ct. at 1741, (quoting *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006)). Such reasoning can be based on interrelated teachings of multiple patents, the effects of demands known to the design community or present in the marketplace, and the background knowledge possessed by a person having ordinary skill in the art. *KSR*, 127 S. Ct. at 1740-41.

## ANALYSIS

### *35 U.S.C. § 103*

Claims 1, 3 through 16, 23 through 25, 28 through 40, 47, and 48

Independent claim 1 recites in relevant part encrypting a title key with a channel-unique key that is produced by combining a channel key and a session key. (App. Br. Appendix A.) Appellants argue that the combination of Richards and Ishiguro does not teach this limitation. (App. Br. 9-10.) Appellants further argue that there is insufficient rationale to combine teachings of the cited references to yield the claimed invention. (*Id.*) In response, the Examiner avers that Richards’s disclosure of a channel control key produced as a result of the combination of a channel access key and

unique encryption variable, taken in combination with Ishiguro's common session keys, teaches that limitation. (Ans. 7, 18-19.)

Therefore, the issue before us is whether one of ordinary skill in the art would have found sufficient rationale to combine Richards' disclosure of a control access key with Ishiguro's disclosure of a session key and a unique key to arrive to the claimed channel-unique key. We answer this inquiry in the affirmative.

As set forth in the findings of fact section, Richards teaches combining a channel access key (CAK) with a user encryption variable (UEV), which replaces a unique customer code to produce a channel control key (CCK), which is subsequently used to produce a program key (PK). (FF 3.) Richards also indicates that all the keys including the CAK change over time. (*Id.*) Further, Ishiguro teaches creating a session key by combining two source session keys. (FF 4.) One of ordinary skill in the art would have readily recognized that the CAK is a session key since, like Appellants' session key, the CAK changes over time. Therefore, the ordinarily skilled artisan would have appreciated Ishiguro's suggestion of combining a session with another key such as Richards' CAK to *predictably result* in the CCK.

Appellants' allegation that there is insufficient rationale to combine the cited references is not persuasive. The Supreme Court has held that in analyzing the obviousness of combining elements, a court need not find specific teachings, but rather may consider "the background knowledge possessed by a person having ordinary skill in the art" and "the inferences and creative steps that a person of ordinary skill in the art would employ." *See KSR Int'l*, at 1740-41. To be nonobvious, an improvement must be

"more than the predictable use of prior art elements according to their established functions." *Id.* at 1740. As set forth in the preceding paragraph, the channel access key and session keys are prior art elements that are being used in a conventional multicast system to perform their established functions to predictably result in a control channel key, which teaches the claimed channel-unique key.

It follows that Appellants have not shown that the Examiner erred in concluding that the combination of Richards and Ishiguro renders independent claim 1 unpatentable.

Appellants allege that the proffered combination does not teach the limitations of claims 5, 9, and 10 through 16. (App. Br. 10-11.) Beyond these mere allegations, Appellants have not presented any evidence or persuasive analysis showing why or how the claimed limitations are patentably distinct from the textual portions upon which the Examiner relies. In our view, such gratuitous allegations are insufficient to overcome the Examiner's *prima facie* case of obviousness. It follows that Appellants have not shown that the Examiner erred in concluding that the combination of Richards and Ishiguro renders the cited claims unpatentable.

Appellants did not provide separate arguments with respect to the rejection of claims 3, 4, 6 through 8, 23 through 25, 28 through 40, 47, and 48. Therefore, we select independent claim 1 as being representative of the cited claims. Consequently, these claims fall together with representative claim 1. 37 C.F.R. § 41.37(c)(1)(vii).

Regarding the rejection of claims 1, 3 through 16, 23, and 47 over Yokota or Knauft in combination with Ishiguro, we agree with the Examiner that Ishiguro teaches producing a session key by combining two other session keys. However, we do not agree with Examiner that Ishiguro's session keys teach or suggest the claimed channel key, which is combined with a session key, to produce a channel-unique key. In our view, Ishiguro's disclosure is simply silent on channel keys. To somehow construe Ishiguro's session key as teaching the claimed channel key without any further evidence to support such equivalency would require us to unreasonably speculate about Ishiguro's disclosure, and to stretch the teachings of the reference beyond reasonable limits. We find that neither Yokota nor Knauft appears to cure the noted deficiencies of Ishiguro. It follows that Appellants have shown that the Examiner erred in concluding that Yokota or Knauft in combination with Ishiguro renders claims 1, 3 through 16, 23, and 47 unpatentable.

#### Claims 41 through 46

##### 1. *New Grounds of Rejection*

Using our authority under 37 C.F.R. § 41.50(b), we reject claims 41 through 46 under 35 U.S.C. § 112, second paragraph.

Independent claim 41 recites in relevant part “means for decrypting...  
...means for deriving...” These phrases are ambiguous. After reviewing Appellants’ Specification, it is unclear to us as to what structures these means correspond to. *See Default Proof Credit Card Sys., Inc. v. Home Depot U.S.A., Inc.*, 412 F.3d 1291, 1298 (Fed.Cir.2005), and *Biomedino*,

*LLC v. Waters Technologies Corp.*, 490 F.3d 946, 950 (Fed.Cir.2007).

Similarly, in claim 44, the logic means for receiving.., the logic means for subscribing.., the logic means for deriving... and the logic means for using... are ambiguous since we could not find corresponding structures for these means in Appellants' Specification. Thus, claims 41 and 44 are indefinite for failing to distinctively claim the subject matter, which Appellants regard as their invention.

Claims 42, 43, 45 and 46 are rejected for fully incorporating the deficiencies of independent claims 41 and 44, by virtue of their dependency thereon.

## 2. 35 U.S.C. § 102

As a consequence of the new ground of rejection above, we pro forma reverse the outstanding prior art rejections of claims 41 through 46 as being anticipated by Richards. The subject matter encompassed by the claims on appeal must be reasonably understood without resort to speculation.

Presently, speculation and conjecture must be utilized by us and by the artisan inasmuch as the claims on appeal do not adequately reflect what the disclosed invention is. Note *In re Steele*, 305 F.2d 859, 862 (CCPA 1962) (A prior art rejection cannot be sustained if the hypothetical person of ordinary skill in the art would have to make speculative assumptions concerning the meaning of claim language.); Note also *In re Wilson*, 424 F.2d 1382, 1385 (CCPA 1970).

3. 35 U.S.C. § 101

Claims 1, 3 and 4 are rejected under 35 U.S.C. § 101 because the claimed invention is directed to non-statutory subject matter. Claim 1, reproduced *supra*, is representative.

Claim 1 is directed to an unpatentable abstract idea because it is neither tied to a particular machine nor operated to change materials to a different state or thing.

“[T]he Supreme Court has held that a claim reciting an algorithm or abstract idea can state statutory subject matter only if, as employed in the process, it is embodied in, operates on, transforms, or otherwise involves another class of statutory subject matter, i.e., a machine, manufacture, or composition of matter. 35 U.S.C. § 101.... Thus, a claim that involves both a mental process and one of the other categories of statutory subject matter (i.e., a machine, manufacture, or composition) may be patentable under § 101.” *See In re Comiskey*, 499 F.3d 1365, 1376-77 (Fed. Cir. 2007)..

“However, mental processes –or processes of human thinking-standing alone are not patentable even if they have practical application.”  
*Id.*

Independent claim 1 recites “[a] method for securely transmitting multicast data”. Claim 1 does not necessarily require a machine, and it does not describe a process of manufacture or a process for the alteration of a composition of matter. In our view, claim 1 merely recites the mental process of manipulating a number to produce another number by the decision of a human. In essence, claim 1 encompasses a human’s ability to use a function in order to encrypt a number, and thus claims the use of mental processes to encrypt the number.

For the above reasons, we find that claims 1, 3, and 4 recite non-statutory subject matter.

II. 37 C.F.R. § 41.50(b)

37 C.F.R. § 41.50(b) provides that, “[a] new ground of rejection pursuant to this paragraph shall not be considered final for judicial review.”

37 C.F.R. § 41.50(b) also provides that the Appellants, *WITHIN TWO MONTHS FROM THE DATE OF THE DECISION*, must exercise one of the following two options with respect to the new grounds of rejection to avoid termination of proceedings (37 C.F.R. § 1.197 (b)) as to the rejected claims:

(1) *Reopen prosecution*. Submit an appropriate amendment of the claims so rejected or new evidence relating to the claims so rejected, or both, and have the matter reconsidered by the examiner, in which event the proceeding will be remanded to the examiner ...

(2) *Request rehearing*. Request that the proceeding be reheard under 37 C.F.R. § 41.52 by the Board upon the same record ...

### III. SUMMARY

- (1) We affirm the Examiner's decision rejecting claims 1, 3 through 16, 23 through 25, 28 through 40, 47, and 48 as being unpatentable over the combination of Richards and Ishiguro.
- (2) We reverse the Examiner's decision rejecting claims 1, 3 through 16, 23 through 23, and 47 over Yokota or Knauft in combination Ishiguro.
- (3) We have entered a new rejection against claims 41 through 46 as being indefinite.
- (4) We pro forma reverse the Examiner's decision rejecting claims 41 through 46 as being anticipated by Richards.
- (5) We have entered a new ground of rejection against claims 1, 3, and 4 as being directed to non-statutory subject matter.
- (6) Because of the new ground of rejections, our decision is not a final agency action.

### DECISION

We affirm the Examiner's decision rejecting claims 1, 3 through 16, 23 through 25, 28 through 40, 47, and 48.

We reverse the Examiner's decision rejecting claims 41 through 46 and enter our own rejection against these claims.

AFFIRMED-IN-PART  
37 C.F.R. § 41.50 (b)

rwk

John L. Rogitz  
Rogitz & Associates  
750 B Street, Suite 3120  
San Diego CA 92101